UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/669,124	09/23/2003	Joel Rosenberger	WIMET121663	2882

26389 7590 02/03/2006

CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER
REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/669,124	**Applicant(s)** ROSENBERGER, JOEL	
	Examiner Christopher A. Revak	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 23 September 2003.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-66* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 23 September 2003 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *see attached*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for domestic priority under 35 U.S.C. 119(e).

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on April 5, 2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-66 are rejected under 35 U.S.C. 102(b) as being anticipated by Whalen et al, US 2004/0003285.

As per claims 1,18, and 34, it is disclosed by Whalen et al of detecting and managing intrusions to a computer network from an unknown wireless source. A security component resides on the network that passively monitors for network traffic received from an unknown wireless device and creates a device profile of the unknown wireless device. It is determined whether the unknown wireless device is an authorized device and if the unknown wireless device is determined to be an authorized device, the network traffic from the unknown wireless device is permitted to pass to the computer network (page 1-2, paragraphs 12-14,16 and page 5, paragraph 46).

As per claims 2,19,43, and 55, Whalen et al teaches that the security component creates a device profile of the unknown wireless device by examining identifying characteristics of the network traffic of the unknown wireless device (pages 1-2, paragraph 12).

As per claims 3,20,35,44, and 56, Whalen et al discloses that the security component creates a device profile of the unknown wireless device by submitting a query to the unknown wireless device and examining the responses received as a result of the query for identifying characteristics of the unknown wireless device (page 2, paragraph 24).

As per claims 4,21,36,34, and 57, it is taught by Whalen et al that the security component creates the device profile of the unknown wireless device by submitting a query to the unknown wireless device based on a characteristic identified in a previously received response and examining the responses received as a result of the query for identifying characteristics of the unknown wireless device (page 2, paragraph 24).

As per claims 5,6,22,2346, and 58, Whalen et al discloses that the characteristic identified in the previously received response is the operating system of the unknown wireless device (page 2, paragraph 24).

As per claims 7,24,47,48,59, and 60, Whalen et al teaches that the identifying characteristics of the unknown wireless device is the MAC address of the unknown wireless device (page 1, paragraph 17).

As per claims 8,25,49,50,61, and 62, it is disclosed by Whalen et al that the identifying characteristics of the unknown wireless device is the TCP/IP address range of the unknown wireless device (page 2, paragraph 24 and page 3, paragraph 35).

As per claims 9,26,37,51, and 63, it is taught by Whalen et al that the query is a standard network query (page 2, paragraph 24).

As per claims 10,27,52, and 64, Whalen et al discloses that the standard network query is a TCP/IP command (page 3, paragraph 35).

As per claims 11,28,53, and 65, it is taught by Whalen et al that the standard network query is a SNMP command (page 3, paragraph 35).

As per claims 12 and 29, it is disclosed by Whalen et al that the network traffic from the unknown wireless device operating in an IEEE 802.11 based wireless network (pages 2-3, paragraph 26).

As per claims 13,14,30, and 38, Whalen et al teaches that the device profile database stores known wireless device profiles and the security component determines whether the unknown wireless device profile is an authorized device by comparing the device profile of the unknown wireless device to device profiles in the device profile database (page 1, paragraph 11 and page 2, paragraph 24).

As per claims 15,31, and 39, it is taught by Whalen et al that if the device profile of the unknown wireless device is not found in the device profile database, the security component associates a threat level with the unknown wireless device according to the unknown wireless device's device profile and network activity (page 2, paragraph 24 and page 4, paragraph 41).

As per claims 16,32, and 40, Whalen et al discloses that the security component de-authorizes the unknown wireless device if the threat level associated with the unknown wireless device exceeds a predetermined threshold (page 4, paragraph 41 and page 5, paragraph 47).

As per claims 17,33, and 41, it is disclosed by Whalen et al that the security component does not permit the network traffic from the unknown wireless device to pass to the computer network if the unknown wireless device is de-authorized (page 1, paragraph 17 and page 5, paragraph 47).

As per claims 42 and 66, the teachings of Whalen et al disclose of detecting and managing intrusions to a computer network from an unknown wireless source. A security component resides on the network that passively monitors for network traffic received from an unknown wireless device and creates a device profile of the unknown wireless device. It is determined whether the unknown wireless device is, or may be, a wireless access point according to the device profile. If the unknown wireless device is, or may be, a wireless access point, the device profile of the unknown wireless device is compared against device profiles of authorized wireless access points to determine whether the unknown wireless device is an authorized wireless access point. If the wireless device is not determined to be an authorized wireless access point, an alert is generated by a system administrator that the unknown wireless device is or may be an unauthorized wireless access point (page 1-2, paragraphs 12-14,16 and page 5, paragraph 46).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
Primary Examiner
AU 2131
1/31/06

CR
January 31, 2006